Matthias Groebel
A Change in Weather (Broadcast Material 1989–2001)
10.12.2022–26.2.2023
Kunstverein für die Rheinlande und Westfalen Düsseldorf

Everything about TV has changed today. What was in the box is obsolete, and what it then displayed has broken free. But the faces have continued to multiply. Now they are available on demand and everywhere, on any device, at any price, in any shape and quality, at any scale, as a thumbnail miniature or a wide screen wall, in any format, setting, preference. Written into Groebel's painted faces is TV as a moment of this history. They draw us in, involving and inviting us to see something of the impact of TV on our sensibilities, its impact on the ways in which look at each other and think about ourselves. They are the messages and media of TV.[1]

– Sadie Plant

Die Ausstellung *A Change in Weather (Broadcast Material 1989–2001)* stellt zum ersten Mal in umfassender Weise die Arbeit des in Köln lebenden Künstlers Matthias Groebel (*1958 in Aachen, DE) vor, der in den letzten fünf Jahrzehnten weitgehend abseits institutioneller Aufmerksamkeit ein einzigartiges und faszinierendes Oeuvre von auf Fernsehbildern basierenden Malereien sowie Fotografien, Videos, Zeichnungen und Recherchearbeiten geschaffen hat. Als ausgebildeter Pharmazeut kam Groebel Anfang der 1980er Jahre als Autodidakt zur Kunst. Zur selben Zeit verbreitete sich das analoge, private Satellitenfernsehen auf breiter Basis in den westdeutschen Privathaushalten und ermöglichte eine vorher nie dagewesene Rund-um-die-Uhr-Verfügbarkeit und einen breiten Zugang zu internationalen Fernsehprogrammen, darunter viele Kanäle ohne deutsche Synchronisierung, deren Kontext und Herkunft für die deutschsprachigen Zuschauer:innen unklar blieben. Groebels Arbeiten aus der Zeit von 1989 bis 2001 reflektieren diese mediale Bedingung des *Open Access Television*, die den gegenwärtigen subskriptionsbasierten, digitalen Streaming-Diensten und dem Pay-TV unmittelbar vorausging und bis heute eine der folgereichsten technologischen Entwicklungen der letzten 50 Jahre bleibt. Obwohl das kalte blaue Flimmern der Kathodenstrahlröhre des analogen Fernsehgeräts längst aus den westlichen Haushalten verschwunden ist, zeichnen Groebels Malereien ein präzises Portrait der Fernsehlandschaft der 1990er Jahre und ihrer spezifischen Mischung aus Voyeurismus, Reality TV, permanenter Selbstinszenierung und Überwachung, die in gewisser Hinsicht das Internet antizipierte.

A Change in Weather (Broadcast Material 1989–2001) fokussiert auf eine Auswahl seiner etwa 200 Malereien aus der Zeit von 1989 bis 2001, die auf appropriierten analogen Fernsehbildern bzw. -stills beruhen und sich von konventioneller Malerei insbesondere durch ihre maschinenunterstützte, in Teilen roboterisierte Produktion unterscheiden: Basierend auf damals neuen Technologien, die analoge Fernseh-Wellensignale in digitale Pixel übersetzen konnten, entwickelte Groebel Ende der 1980er Jahre eine Maschine, mit deren Hilfe er Stills aus dem laufenden Fernsehen nachträglich mit einer Airbrush-Pistole und einem mehrstufigen, komplexen Farbauftrag auf Leinwand übertragen konnte – rund ein Jahrzehnt, bevor der erste Farb-Plotter für eine breite Masse an privaten Konsument:innen verfügbar wurde. Angepasst auf die maximale Bildfläche, die die Maschine auf Leinwand bringen konnte, sind Groebels Bildformate mit wenigen Ausnahmen auf eine quadratische Einheitsgröße von 95 × 95 cm skaliert. Auf den Folgeseiten dieses Booklets sind Abbildungen der Maschine abgedruckt.

Everything about TV has changed today. What was in the box is obsolete, and what it then displayed has broken free. But the faces have continued to multiply. Now they are available on demand and everywhere, on any device, at any price, in any shape and quality, at any scale, as a thumbnail miniature or a wide screen wall, in any format, setting, preference. Written into Groebel's painted faces is TV as a moment of this history. They draw us in, involving and inviting us to see something of the impact of TV on our sensibilities, its impact on the ways in which look at each other and think about ourselves. They are the messages and media of TV.[1]

—Sadie Plant

A Change in Weather (Broadcast Material 1989–2001) is the first comprehensive exhibition of the work of the Cologne-based artist Matthias Groebel (b. 1958 in Aachen, DE). Over the past four decades, and largely without institutional recognition, Groebel has created a unique and fascinating oeuvre featuring paintings based on images from television, along with drawings, photographs, videos, and research works. As a trained pharmacist, Groebel came to art in the early 1980s as an autodidact. It was during this period that private analog satellite television spread throughout West German households, allowing unprecedented round-the-clock access to a wide range of international television programs, including many undubbed foreign channels whose contexts and origins remained opaque to German-speaking audiences. Groebel's works from 1989 to 2001 reflect this new media condition of open-access television, which directly paved the way for the subscription-based streaming and pay-per-view services of today and still counts as one of the most influential technological developments of the last 50 years. While the cold blue flicker of cathode-ray tube televisions has long disappeared from Western households, Groebel's paintings offer a precise portrait of the televisual landscape of the 1990s and its specific mixture of voyeurism, reality TV, permanent self-staging, and surveillance, all of which anticipated the internet to a certain extent.

A Change in Weather (Broadcast Material 1989–2001) focusses on a selection of the roughly 200 paintings Groebel produced between 1989 and 2001. All based on appropriated analog television stills, the works differ from conventional paintings primarily in their machine-assisted and partly robotized production process. In the late 1980s, Groebel utilized new technology capable of translating analog television signals into digital pixels to develop a machine that allowed him to transfer images from the television onto canvas, a complex process involving multiple stages and applications of paint with an airbrush pistol – and this around a decade before the first color plotter was made available to a wide range of private consumers. Adjusted to the maximum surface area the machine was capable of creating on canvas, the vast majority of Groebel's paintings were produced in a square format of 95 × 95 cm. Images of the machine can be found on the following pages of this booklet.

Groebel's production process played on a reciprocal and closely intertwined relationship between artist/painter, technology, and generative form-finding in an era of profound technological change and the digital turn. His works arose from the need for a form of painting that was not limited to just symbolically depicting the techno-cultural changes of the period, but which could

Groebels Produktionsprozess spielt auf ein wechselseitiges, eng verwickeltes Verhältnis zwischen Künstler:in/Maler:in, Technologie und generativer Formfindung in einer Zeit des tiefgreifenden technologischen Wandels und der digitalen Wende an. Seine Arbeiten entstanden aus dem Bedürfnis nach einer Malerei-Praxis, welche die techno-kulturellen Veränderungen ihrer Zeit nicht nur symbolisch abbildet, sondern diese auch auf struktureller, medialer Ebene reflektieren, in sich aufnehmen, verarbeiten und transformieren kann. Seine Malereien basieren auf damals allgegenwärtigen medialen Bildern – generisch und gleichzeitig hochgradig konnotiert –, und haben dadurch wie er selbst sagt „auch dann einen Effekt, wenn Du es gar nicht willst". Durch Groebels bewusste Abkehr von einer konventionellen malerischen Bildfindung, die sich bis heute meist durch individuelle Autor:innenschaft und subjektiven Ausdruck („Authentizität") definiert, wirken seine Malereien retrospektiv auf radikale Weise ihrer Zeit voraus. Sie entstanden in einem mehrstufigen Prozess der Auftragserteilung an die Maschine (Einspeisung von Information), der Aufgabe von künstlerischer Kontrolle und des kontinuierlichen Eingreifens, Überarbeitens und Manipulierens der resultierenden Bilder. Dieser konstante künstlerische Dialog mit dem, was die Maschine hervorbrachte, und die Einbindung von Zufällen und Fehlern in den künstlerischen Prozess lässt die klare Unterscheidung zwischen Information und malerischer Geste sowie massenmedialem (kollektiven) und künstlerischem (subjektivem) Signal zunehmend obsolet erscheinen.

Groebels Arbeiten vermitteln ein Gefühl für die hypnotischen Erfahrungsräume des analogen Fernsehens, für die flackernden, von hinten beleuchteten und verschwommenen Mosaik-Bilder, die aus bewegten Licht-Elektroden bestanden und sich erst auf der Retina der Zuschauer:innen zu einem Bild zusammenfügten.[2] Seine Bilder konfrontieren uns auf direkte, manchmal abrupte Weise mit einem Übermaß an sprechenden Köpfen und Nahaufnahmen von Körpern und Körperteilen und damit auch mit der grenzüberschreitende Intimität des Fernsehens. Im Unterschied zum unerreichbaren Hollywood-Filmstar auf Zelluloid suggerierte das Fernsehen eine vertraute öffentliche Persönlichkeit – eine Art sehende, sprechende Oberfläche, die einen zu Hause direkt aus dem Gerät heraus anblickte.[3] Groebels Portraits spielen mit dieser vermeintlichen Vertrautheit; einmal meint man den Frontsänger der britischen New Wave-Band The Cure zu erkennen, ein anderes Mal ist es der normierte Look der 90er Jahre, der eine Person aussehen lässt wie eine:n Freund:in aus der Zeit, letztlich bleiben die Bilder aber generisch und anonym. Zugleich haben sie eine mysteriöse körperliche Präsenz und eine große psychologische Unterschwelligkeit, die undefiniert lässt, von welchen Kräften und Motiven die portraitierten Personen und Körper gesteuert werden. Verhältnisse von Kontrolle, Überwachung, Entblößung, Voyeurismus, Unbehagen und körperlicher Hingabe sind abwechselnd angedeutet, aber nie ausformuliert. Die mysteriöse Latenz der Bilder hat auch mit den Nischenprogrammen und deren Inhalten zu tun, aus denen Groebel oft schöpfte, und die in den Anfängen des privaten Fernsehens weit nach Mitternacht abseits von staatlicher und redaktioneller Kontrolle und der Konsenskultur des öffentlich-rechtlichen Rundfunks zirkulierten. Groebels Bilder arbeiten die Suggestivkraft und

reflect, incorporate, process, and transform them on a structural level. The paintings are based on what were ubiquitous images in the media of the time—simultaneously generic and highly suggestive—and have, as the artist himself says, "an effect, even when you don't want them to." Groebel's conscious departure from a more conventional approach to painting, which even today is defined largely by ideas of individual authorship and subjective expression ("authenticity"), makes his paintings seem radically ahead of their time when viewed in retrospect. They are the products of a multi-stage process of issuing commands to a machine (feeding it information), surrendering artistic control, and continuously intervening in, reworking, and manipulating the resulting images. This constant artistic dialog with the output of the machine, and the inclusion of errors and chance in the artistic process, makes the clear distinction between information and painterly gesture, and between the collective and subjective signals of mass-media and art, seem increasingly obsolete.

Groebel's works convey a feeling for analog television's hypnotic spaces of experience; for the flickering, backlit, and low-resolution images that moving electrons produced on the screen, only forming discernible content once they reached viewers' retinas.[2] They directly and at times abruptly confront us with an abundance of talking heads and close-ups of bodies and body parts, and hence with the transgressive intimacy of television. Where the Hollywood star on celluloid seemed unreachable, television projected a sense of familiarity and openness—a sort of seeing, speaking surface that looked out at us in our homes from within the device.[3] Groebel's portraits play with this seeming familiarity: at one point it seems as if the frontman from the British new-wave band The Cure can be made out, at another it's someone with the same standardized '90s look of a friend from the time; ultimately, though, the images remain generic and anonymous. At the same time, they have a mysterious physical presence, with a powerful sense of psychological latency that leaves open the question of what forces and motives are governing these people and bodies. Conditions of control, surveillance, exposure, voyeurism, unease, and bodily abandon are all implied at points, but never made explicit. The mysterious power that seems to be concealed within these images is also due to the niche programs Groebel often drew from, whose contents were frequently aired way past midnight back in the early days of private television, beyond state or editorial control and the consensus culture of public service broadcasting. Groebel's images bring out the suggestive power, latent tensions, and power structures inherent within a gesture, a gaze, or the biting of nails, often contrary to the intrinsic and profit-driven agendas of the entertainment industry. His paintings are frequently subtle manipulations or *détournements* of the source material.

If the term "rabbit hole" now describes the pull and manipulative power of digital media, in the 1980s and 1990s it was instead the trancelike flicker of the television screen, the blue light of the cathode-ray tube, and the fuzziness of the image it produced that all had a similarly immersive effect on viewers. This shimmering, hallucinatory quality is mirrored in Groebel's paintings, lending them a somnambulistic presence. They allow us to reflect on the beginnings of our digital culture and media landscape, which has long determined our phys-

die unterschwelligen Spannungen und Machtstrukturen heraus, die einer Geste, einem Blick oder einem Nagelkauen eigen sind, oft konträr zu den originären und profitgetriebenen Absichten der Unterhaltungsindustrie. Groebels Malereien sind oft subtile Manipulationen oder *Détournements* des Ausgangsmaterials.

Wenn heute der Begriff des *Rabbit Hole* die Sogwirkung und Manipulationsfähigkeit digitaler Medien bezeichnet, dann war es in den 1980er und 1990er das trancehafte Flimmern des Fernsehers, das blaue Licht der Kathodenstrahlröhre und die Unschärfe des Bilds, die eine ähnlich immersive Wirkung auf die Zuschauer:innen ausübten. Diese flirrende, halluzinatorische Qualität spiegelt sich in Groebels Malereien und gibt ihnen eine traumwandlerische Präsenz. Sie lassen uns über die Anfänge unserer digitalen Kultur und Medienlandschaft nachdenken, die längst auch unser physisches Leben bestimmt und deren psychologischen Effekten wir uns nur schwer entziehen können. Die Ausstellungsarchitektur greift den Gedanken des Sogs und der Überinformation auf und zeigt Groebels Malereien auf Wänden, die in die Tiefe des Ausstellungsraums gestaffelt sind. Die Leinwände werden nie autonom, sondern in Rastern gezeigt, um einen assoziativen Bogen zu Medienarchiven und kollektiv gespeichertem Wissen zu spannen; zur „psychischen Tiefe unseres medial Unbewussten“[4].

Der Künstler Andreas Selg, der als Co-Kurator für die Ausstellung eingeladen wurde, hat seit 2021 zwei Ausstellungen von Groebel in Galerien in Köln und Zürich organisiert. Sein Interesse gilt der Rekonfiguration einzelner Werkgruppen und der Rekontextualisierung von Groebels Oeuvres vor dem Hintergrund zeitgenössischer Kunstdiskurse. Selg ist Mitherausgeber der neu erscheinenden Monografie zu Groebel.

Kuratiert von Kathrin Bentele und Andreas Selg

1 Sadie Plant, „Painted Faces“, in: *Matthias Groebel:Painted Faces. Broadcast Material 1989–2006*, hrsg. von Andreas Koller und Andreas Selg, Edition Patrick Frey, Zürich, 2022, S. 220.
2 Vgl. Andreas Selg, „The Image-Sweep“, in: *Matthias Groebel: Painted Faces. Broadcast Material 1989–2006*, hrsg. von Andreas Koller und Andreas Selg, Edition Patrick Frey, Zürich, 2022, S. 11–12.
3 Vgl. Sadie Plant, „Painted Faces“, in: *Matthias Groebel: Painted Faces. Broadcast Material 1989–2006*, hrsg. von Andreas Koller und Andreas Selg, Edition Patrick Frey, Zürich, 2022, S. 16.
4 Vgl. Andreas Selg, „The Image-Sweep“, in: *Matthias Groebel: Painted Faces. Broadcast Material 1989–2006*, hrsg. von Andreas Koller und Andreas Selg, Edition Patrick Frey, Zürich, 2022, S. 10.

ical lives and whose psychological effects seem hard to escape. The exhibition architecture takes up the idea of being pulled in, and of information overload, by displaying Groebel's paintings on walls stacked deep into the exhibition space. The canvases are not shown autonomously but in grids, evoking associations with media archives and collectively stored knowledge—in other words, the "collective psychic depth of the medial unconscious."[4]

The artist Andreas Selg, who was invited to co-curate the exhibition, has organized two exhibitions of Groebel's work since 2021, in galleries in Cologne and Zürich. His interest is in the reconfiguration of individual groups of works and the recontextualization of Groebel's oeuvre against the backdrop of contemporary artistic discourses. Selg is also co-editor of the newly published monograph on Groebel.

Curated by Kathrin Bentele and Andreas Selg

1 Sadie Plant, "Painted Faces," in: *Matthias Groebel: Painted Faces. Broadcast Material 1989–2006*, eds. Andreas Koller and Andreas Selg, Edition Patrick Frey, Zürich, 2022, p. 220.
2 See Andreas Selg, „The Image-Sweep", in: *Matthias Groebel: Painted Faces. Broadcast Material 1989–2006*, eds. Andreas Koller and Andreas Selg, Edition Patrick Frey, Zürich, 2022, pp. 11–12.
3 See Sadie Plant, "Painted Faces," in: *Matthias Groebel: Painted Faces. Broadcast Material 1989–2006*, eds. Andreas Koller and Andreas Selg, Edition Patrick Frey, Zürich, 2022, p. 16.
4 See Andreas Selg, "The Image-Sweep," in: *Matthias Groebel: Painted Faces. Broadcast Material 1989–2006*, eds. Andreas Koller and Andreas Selg, Edition Patrick Frey, Zürich, 2022, p. 10.

Begleitprogramm

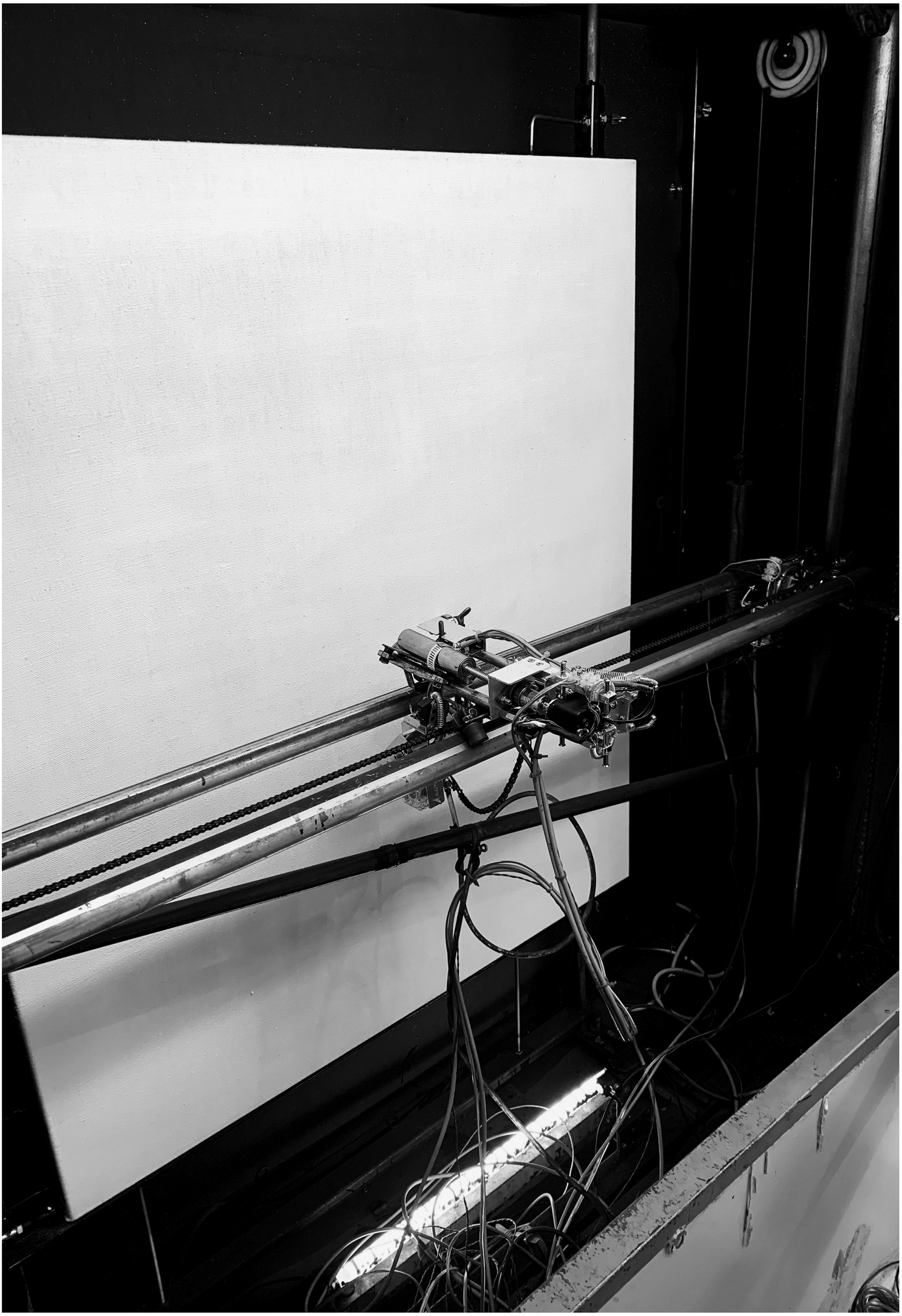
Am Wochenende des 4. und 5. Februar 2023 laden wir im Rahmen der Einzelausstellung von Matthias Groebel zu einem mehrteiligen Begleitprogramm in den Kunstverein ein.

Das Programm beinhaltet einen Beitrag der britischen Kulturtheoretikerin Sadie Plant (*1964 in Birmingham, UK, lebt und arbeitet in Biel, CH), die u.a. durch ihre Bücher *Writing on Drugs* (1997); *Zeros and Ones: Digital Women and the New Technoculture* (1997) oder *The Most Radical Gesture: The Situationist International in a Postmodern Age* (1992) bekannt geworden ist. Der deutsche Autor und Künstler Hans-Christian Dany (*1966 in Hamburg, DE, lebt und arbeitet in Hamburg, DE) wird ebenfalls einen neuen Beitrag vorstellen. Zu Danys Veröffentlichungen gehören u.a. *MA-1. Mode und Uniform* (2018); *Morgen werde ich Idiot. Kybernetik und Kontrollgesellschaft* (2013) oder *Speed. Eine Gesellschaft auf Droge* (2012). Ebenfalls findet ein Performance-Konzert des US-amerikanischen Experimentalmusiker-Duos Jack Callahan (*1990, US, lebt und arbeitet in New York, US) und Jeff Witscher (*1984 in Long Beach, US, lebt und arbeitet in New York, US) statt.

Accompanying program

On the weekend of February 4 and 5, 2023, the Kunstverein will host a program of events to accompany Matthias Groebel's solo exhibition.

The program includes a contribution by the British cultural theorist Sadie Plant (b. 1964 in Birmingham, UK, lives and works in Biel, CH), known for her books *Writing on Drugs* (1997), *Zeros and Ones: Digital Women and the New Technoculture* (1997), and *The Most Radical Gesture: The Situationist International in a Postmodern Age* (1992). The German author and artist Hans-Christian Dany (b. 1966 in Hamburg, DE, lives and works in Hamburg, DE) will also present a new contribution. Dany's publications include *MA-1. Mode und Uniform* (2018), *Morgen werde ich Idiot. Kybernetik und Kontrollgesellschaft* (2013), and *Speed. Eine Gesellschaft auf Droge* (2012). In addition, there will also be a performance-concert by the US-based experimental musical duo Jack Callahan (b. 1990 in the US, lives and works in New York, US) and Jeff Witscher (b. 1983 in Long Beach, US, lives and works in New York, US).



DYNAMIXEL
MX-12W

→

Auf den folgenden Seiten ist ein Auszug aus Matthias Groebels *Hacked Channels. User's Manual* (1999) abgedruckt. Anfang der 2000er Jahre gingen private Fernsehstationen auch in Deutschland dazu über, nur noch kostenpflichtig und auf Subskriptionsbasis Fernsehangebote zur Verfügung zu stellen und verschlüsselten ihre Inhalte. Groebel benutzte in Reaktion darauf ein analoges Codiersystem, um weiterhin Zugang zu diesen Fernsehbildern zu haben. Die resultierende Malerei-Serie *Hacked Channels* basiert auf solchen „gehackten" Fernsehbildern, bei denen die analoge Dekodierung nicht vollumfänglich glückte und die ein Hybrid aus Signal und decodiertem Bild darstellen. *Hacked Channels. User's Manual* ist eine Anleitung zur Dekodierung, die damals in Hacker-Kreisen zirkulierte.

→

The following pages present an excerpt from Matthias Groebel's *Hacked Channels. User's Manual* (1999). In the early 2000s, private television channels in Germany followed those in other countries by moving to a paid subscription model, subsequently encrypting their content. In reaction to this, Groebel began using an analog coding system in order to have continued access to these channels and their images. The resulting series of paintings, *Hacked Channels*, is based on these "hacked" images, in which the analog decoding was only partially successful, producing hybrids made up of signal and decoded image. *Hacked Channels. User's Manual* is an instruction manual for decoding these signals that circulated among hackers at the time.

Some technical details about Videocrypt

In this file, I'll collect some of the details known or assumed about the Videocrypt pay-TV access control system. Consider it as some kind of frequently asked questions list with answers about the system.

1. Basic Principle

Videocrypt encodes the TV image by cutting each line of the image in two pieces at some cut point and then exchanges these two line fragments in the broadcasted pictures. E.g. if a line like

0123456789

passes the encoder, the output might look like

4567890123

where the digits represent the pixels of the image. There are 256 possible cut points and there are no cut points directly near the image border (the miniumum distance from the margin is about 12-15% of the image width) which is the reason why you sometimes still can see vertical patterns even on an encrypted image. The sound is currently not encrypted.

Several times per second, a computer at the broadcasting station generates a 32 byte long message which is broadcasted encoded together with forward error correction information in the first invisible lines of the TV signal similar to teletext. About every 2.5 seconds, one of these 32-byte messages is processed in the encoder by a secret hash algorithm which transforms the 32-byte message into a 60-bit value. These 60 bits are then used by a second algorithm in order to determine the 8-bit cut point coordinates for each line for the next 2.5 seconds. No details about this second algorithm are known, but think of it just as some kind of 60-bit pseudo random number generator (PRNG) were the 60-bit output from the secret hash function is used as a start value (seed).

The decoder receives the 32-byte messages and other data together with the TV signal, applies some error correction algorithms and passes all 32-byte messages to the smartcard in the decoder's card slot. The smartcard implements the same secret hash function and answers with the same 60-bit value as the one which is used in the encoder. By using this 60-bit answer from the card, the decoder hardware can generate with the same PRNG the same cut point sequence as the encoder and can so reconstruct the original image by again exchanging the two line fragments. The secret hash function is a cryptographically strong system which is designed so that it is extremely difficult to guess the algorithm of this function by looking at many pairs of 32-byte/60-bit values.

Apart from providing the source for the generation of the 60-bit PRNG seeds, the 32-byte messages from the broadcasting station contain card numbers so that individual cards can be addressed and they contain commands like activation, deactivation, or show-a-message for the addressed card. In addition, the 32-byte packets contain a digital signature (currently 4 bytes) that allows the card to test whether the 32-byte messages really originate from the encoder and have not been generated by someone analysing the card. Again, this digital signature like the hash function has been designed so that it is difficult to find out how to generate a correct signature by looking at enough examples. This prevents choosen-text attacks, where someone tries to probe the secret hash function with very carefully selected 32-byte messages and this prevents hackers to generate new activation commands for the card.

In early 1993, someone managed to get access to the secret hash functions of several stations which use Videocrypt (e.g., British Sky

Broadcasting, Adult Channel, JSTV, BOB, Red Hot TV). All these systems used the same hash and signature algorithm and the only difference between the stations was a 32-byte secret key table. It is not known how it was possible to get this information. Either someone from the company who manufactured the cards (News Datacom) released this information or it was possible for someone to read out the EPROM contents of the card processor (less likely, but also theoretically possible). With this knowledge it was then quite easy possible for the original hackers to produce 'clone cards'. These are simple PCBs with a cheap microcontroler (e.g. one of Microchip's PIC family), which implements only the secret hash function and serial I/O procedures in its EPROM and answers with the correct 60-bit values to 32-byte messages just as the real cards do. For several channels, clone cards are still available, but BSkyB distributed new 09 series cards in spring 1994 and switched on 1994-05-18 to a new secret hash function. Consequently, all clone cards stopped to work. It is not known whether only the secret 32-byte key was changed, or whether also the hash and/or signature algorithm have been modified. Even if the algorithm is still the same it is extremely difficult to find out the new 32-byte key table.

The clone cards didn't implement any interpretation procedures for card activation or deactivation and pay-per-view functions, so their software is considerably simpler than the one in the real cards. This results in some tiny differences between the reaction of the clone card software and the reaction of the original card software on pathological 32-byte messages. These differences were used in counter measures against clone cards several times in 1993 and 1994 by BSkyS in order to deactivate clone cards, but it was quite easy each time to find out these tiny bugs in the clone card software and correct it.

There is an Intel 8052 microcontroler in the decoder which manages the communication between the smart card and the rest of the system. As the software of this processor is not read protected, it was also possible to reprogram this chip (by using the EPROM version 8752BH) so that the hash algorithm is performed inside the decoder. Then no external card is needed at all for the channels for which the hash algorithm was implemented in the 8752.

More detailed basic information about Videocrypt has been published in the European patent EP 0 428 252 A2 ("A system for controlling access to broadcast transmissions"). You can order a copy for a little money from the European Patent Office if you are interested.

2 Security of the Videocrypt system

The system is very secure, because all secret parts that are essential to a successful decryption are located in the smart card and if the card's secret hash algorithm/key becomes known, it can easily be replaced by just sending new cards to the subscribers. This card exchange can also be used if details about the format of the commands hidden encrypted 32-byte sequences sent to the card become known.

There are however at least two obvious security flaws of the system which can't be removed by new smart card generations:

- The dialog between the card and the decoder is the same synchronously for all Videocrypt decoders switched to this channel. I.e., the decoder doesn't add any card specific or decoder specific information to the traffic. This makes it possible to use one card for several decoders. E.g. it is possible to record the 32-byte messages broadcasted by the station during an evening with a PC, then send these messages to someone else with an original card who asks his card for the 60-bit answers to all the recorded messages. If this person then sends these 60-bit answers back, then you can use this data in order to descramble the VCR recorded program of this evening (delayed data transfer). However, decoding VHS recorded encrypted signals produces

minor color distortions and a few VCRs don't preserve the Videocrypt data stream in the first invisible lines that accompanies the TV signal. It is also possible to distribute the card answers from one card in real-time with cables to many decoders in a house or with radio signals to many decoders in a larger region.

- The simple cut-and-exchange encryption method and the fact that two consecutive lines in an image are almost always nearly identical makes it possible to try out all possible combinations and to select the one which causes both lines to fit together best. This method has alreday been implemented on fast PC's with framegrabbers which load the image into the memory and display it corrected on the computer screen (many seconds per frame), on parallel supercomputers which allow almost real-time decryption and with special hardware that achieves real-time decryption. However, with this decoding method, there are severe image quality losses and many additional problems which together with the high hardware costs required (much higher than a regular subscription) don't make this approach very practical for every day usage.

Both these security gaps in the videocrypt systems don't allow comfortable and easy high quality decryption like using a card, but the described methods have already been successfully used by a few technically skilled peoples for watching encrypted program.

3 ISO card protocol

The card and the protocol used to cummunicate with it conform exactly to the international standard ISO 7816. The options used from this standard are: T=0 asynchronous half duplex character transmission protocol, active low reset and inverse convention. Only a few basic principles of the ISO protocol will be explained here. For much more detailed information, please read the ISO standard which you can order from your national standards body (e.g. DIN, ANSI, AFNOR, BSI, DS, etc.). There are three parts of the standard: ISO 7816-1 describes physical characteristics of the card and quality requirements the card has to survive, ISO 7816-2 describes the location and meaning of the contacts and ISO 7816-3 (most important) describes the electrical characteristics, the answer-to-reset message and the protocol.

The data format is an asynchronous 9600 bit/s serial format similar to that used on RS-232 lines, with 8 data bits, 1 parity bit and two stop bits. The parity is even (but if inverse bit meaning convention is used, a RS-232 interface has to be programmed for odd parity in order to produce the correct bit). There is also an error detection and character repetition mechanism in the protocol which is not supported by RS-232 interfaces: If the receiving device (card or decoder) detects a parity error, it sends an impulse during the stop bit time. This will tell the sender to retransmit one byte.

After a reset impulse to the card, the card answers with an answer-to-reset message with some information about the requirements of the card. If the first byte is 0x3f, then this means that in order to read the bytes with a RS-232 interface, you'll have to invert and reverse all bits. A typical answer-to-reset looks e.g. like the following one:

```
    3f fa 11 25 05 00 01 b0 02 00 00 4d 59 00 81 80
    |  |  |  |  |  | | historical characters, card
    |  |  |  |  |  | | information about chip and
    |  |  |  |  |  | | software version, etc.
    |  |  |  |  |
    |  |  |  |  +- low nibble: protocol type T=0,
    |  |  |  |     high nibble: end of ISO part
    |  |  |  +- requests 5 additional stop bits
    |  |  |
    |  |  +- encodes programming voltage and max. programming
```

```
          |  |     current (here: 5V, 50mA)
          |  |
          |  +- clock freq.: 00h=3.5MHz, 31h=7 MHz
          |
          +- the 0ah low nibble means: 10 'historic characters' which
             are not defined in the ISO standard are appended to
             the reset answer
```

The answer-to-reset message has a variable length format. Some bits specify whether certain bytes are present or not. If the lowest bit in the high nibble of the second byte is 1, then the above shown third byte is present and determines the relation between the bit rate and the clock frequency after the reset answer. E.g., 11h means that 372 clock cycles are one bit duration (default), i.e. with a clock frequency of 3.5712 Mhz, the bit frequency is 9600 Hz. In the Videocrypt system, the bit rate is always 9600 bits/s, but a value of 31h (= factor 744) in the third byte requests a doubled clock frequency (~7MHz) from the decoder. Other values are not supported by the Videocrypt decoder.

The Videocrypt decoder supports several programming voltages (5 V, 12.5 V, 15 V and 21 V, max. 50 mA current) and different numbers of stop bits (>= 5) sent to the card. All these parameters can be selected in the answer-to-reset. Of the 'historic characters' part, the decoder only verifies that it is at least 7 characters long and that the values 4dh, 00h, 00h at the positions 4 to 6 in the example. Otherwise, the card is rejected. No more details about the information in the historic characters part of a Videocrypt card is currently known. For the detailed format of the answer-to-reset message, please consult ISO 7816-3.

The T=0 protocol is a half duplex master slave protocol. The decoder can send commands to the card followed by a data transmission either to or from the card. The card can do some limited flow control and can request or deactivate the programming voltage VPP selected in the answer-to-reset using "procedure bytes". If the decoder initiates a command, it sends five header bytes to the card, e.g.:

```
53 78 00 00 08
```

The first byte (CLA) is the command class code and is always 53h in the Videocrypt system. The second byte (INS) is the instruction code. Its lowest bit is always 0 and Videocrypt instruction codes have always a 6 or 9 high nibble (you'll see below, why). The following 2 bytes (P1 and P2) are a reference (e.g. an address) completing the instruction code and a Videocrypt decoder sets them always to 00 00. The final byte (P3) codes the number of data bytes which are to be transmitted during the command. P3=0 has a special meaning. In data transfers from the card, it indicates 256 data bytes, in data transfers from the decoder, it indicates 0 bytes. The direction of the data transfer is determined by CLA and INS and must be known in advance by both the card and the decoder.

After transmission of such a 5 byte header, the decoder waits for a 'procedure byte' from the card.

The following procedure bytes are possible:

60h	Please wait, I'll send another procedure byte soon, don't timeout.
INS	Now let's transfer all (remaining) data bytes, I don't need programming voltage.
INS+1	Now let's transfer all (remaining) data bytes and please activate VPP.
INS xor ffh	Now let's transfer another single data byte, I don't need programming voltage.

(INS+1) xor ffh	Now let's transfer another single data byte, and please activate VPP.
6Xh or 9Xh	This byte SW1 indicates an end of the data transfer and requests to deactivate VPP. A second status byte SW2 follows from the card. SW1 SW2 = 90 00 indicates a normal termination, other values report e.g. an error.

After each data transfer, the decoder waits for another procedure byte. E.g., a typical decoder<->card dialog looks like this (command 78h requests the 60-bit answer as 8 bytes from the card):

```
decoder sends header
  53 78 00 00 08
card sends procedure byte (all at once, no VPP)
  78
card sends P3 data bytes
  80 52 02 79 f5 39 7c 0e
card finishes with SW1 and SW2
  90 00
```

4 Videocrypt protocol

The newer Videocrypt smart cards don't require any programming voltage. Although, the ISO standard requires only 2 stop bits after each transferred byte, Videocrypt decoders seem to require more than 5 stop bits. As PC serial ports don't support more than 2 stop bits directly, a card emulator software has to wait for about 0.5-1.5 ms after each byte. Cards may announce in the answer-to-reset message how many stop bits they require.

A videocrypt decoder knows the following 10 commands (all with CLA=53h and P1=P2=00h):

INS	length (P3)	direction	purpose
70h	6	from card	serial number, etc.
72h	16	to card	message from previous card
74h	32	to card	message from station
76h	1	to card	authorize button pressed
78h	8	from card	60-bit answer
7ah	25	from card	onscreen message
7ch	16	from card	message to next card
7eh	64	from card	???
80h	1	to card	???
82h	64	from card	???

The following things are known about the data bytes of these commands:

70h:

In BSkyB cards, the 70h data contains the card serial number (e.g. 06 09) in the low nibble of the first byte. The high nibble of the first byte seems to be always 2. The next 4 bytes form an 32-bit bigendian integer value which corresponds to the decimal card number without the final digit of the card number (which is perhaps a check digit, algorithm unknown). The meaning of the final byte is unknown.

72h and 7ch:

Several times per second, the decoder requests with 7ch 16 bytes from the card. If a card is removed and a new card is inserted in the decoder without switching off the power of the decoder, then shortly after the card reset, the decoder sends the latest 7ch data bytes from the previous card in a 72h message to the new card. In this way, 16 bytes information (e.g. the status of a pay-per-view account or a list

of activated channels?) can be transfered from one card to the next.

74h and 78h:

The 74h command transfers the 32-byte messages from the broadcasting station to the card. If the third bit (value 8) in the first byte is set, then the decoder will ask with a 78h command for the 60-bit answer. This happens about every 10 74h packet every 2.5 seconds. The high nibble of the final byte in the 78h data is ignored by the decoder (only 60 bits are needed). The high nibble of the first 74h byte seems to have the value eh or fh in normal encrypted operation and ch or dh in the 'soft scrambled' mode where the decoder can descramble the image even without any card.

The following information is valid for the 07 BSkyB card and need not necessarily be true for future smart cards, because these data bytes don't seem to be interpreted in the decoder and so their meaning can be exchanged. A typical BSkyB 74h packet for the 09 series card looks like this:

e843 0a888261 0c 29e403f6 20202020202020202020202020202020 fb54ac02 51

The second byte selects one of several 32-byte secret key tables that are used by the hash function. When the switchover from the 07 cards to the 09 cards happened, this value increased from 40h to 43h. In the 07 card, this value was only interpreted to find an offset into a table with various 32-byte secret keys. The lower 7 bits of the seventh byte contain a channel ID. The final byte 32 is a simple checksum that makes the sum of all 32 bytes a multiple of 256. The 4 bytes 28-31 contain the digital signature that is simply an intermediate result of the iterations of the hash algorithm. If the checksum, the digital signature, or some of the values in the first 7 bytes of a 74h command aren't correct, then the 78h answer will only contain 8 00 bytes or in some cases 01 00 00 00 00 00 00 00. The 07 card had an interesting security flaw: the card sends to the decoder as many data bytes as specified in P3. By sending a higher length value in the command header to the card, one can get up to 256 data bytes back which seem to be values from the card's RAM that allow some insight into the internal data structures of the card software.

The following theory has been proposed about the encoding of the card addresses, but this hasn't been verified yet and might be partially or completely wrong: A card number is perhaps represented by a 5 byte card address consisting of a 4 byte prefix and a 1 byte suffix. Up to 16 cards with the same card address prefix can be addressed with one 32-byte message. The bytes 0-11 might contain the common prefix to the addressed cards and the bytes 12-27 the various suffixes. If there are less than 16 different cards to be addressed, then the same suffix byte is repeated several times in order to fill the space. There's no good theory about the meaning of the 4 bytes 3-6. E.g. the command which is sent to the card could be encoded here, but no contents are known and as these bytes seem to have pretty random values, it is possible that some of these are random bytes or time stamps and that the other bytes are encrypted with e.g. intermediate values of the hash function (like the signature).

76h:

If the authorize button on the decoder is pressed for a few seconds, then the decoder will send a single 76h message with a 00 data byte to the card.

7aH:

This command requests from the card an ASCII text which is then displayed on the TV screen. The display field is 12 characters wide,

one or two lines high and no lowercase letters are supported. The lower 5 bits in the first byte indicate, how long the text is which is to be displayed (0 = no display). Probably a single line can be for 2 lines. The highest 3 bits of the first byte seem to be some kind of display priority. The number there (0-3) must be high enough if standard decoder messages have to be suppressed. The remaining 24 bytes contain the ASCII test.

The meaning of the other commands is unknown, some of them are never used currently. Some cards understand also additional instruction codes which can't be issued by a normal decoder. E.g. a BSkyB 09 card understands also 12h, 86h, 88h, 8ah and 8ch. These commands are perhaps used in order to test or configurate the card at the factory, etc.

Please contact me if you find out anything new. My e-mail address is mskuhn@cip.informatik.uni-erlangen.de.

5 VCL File Format

The Videocrypt Card Logfile format (VCL) is used by some peoples for performing the delayed data transfer procedure described in section 2. Person A with a valid card can record the dialog between the decoder and the card for a certain program P and transmit this information as a VCL file to person B who has no card and has recorded with a VCR only the encrypted signal of program P. Person B now connects the Videocrypt decoder between the VCR and the TV set and connects the card slot of the decoder to a PC. Using the information in the VCL file, B's computer can now also decrypt program P. This is of course only possible for the few hours which are covered by the information in the VCL file.

Not all of the information exchanged between the card and the decoder is necessary for descrambling the TV signal. The VCL format uses this fact in order to save a lot of storage space. Only 12 bytes of high entropy (that means: almost uncompressable) are stored every 2.5 seconds. So a VCL file of a 1 hour program is only about 17 kbytes large. In addition, VCL files don't contain any information about the card owner (especially not the card serial number), which appears in normal full log files. (The only potential security hole is the remaining 4 bytes in the 78h command. Consequently, they should be cleared in order to avoid card specific information to leak into the VCL file.)

VCL files have a very simple binary format consisting of a 128 byte header and arbitrarily many 12 byte records. At the end, VCL files may be padded with zero bytes to a multiple of the operating system's disk sector size, so that no RAM contents can leak in there out of an unsecure system like MS-DOS. Don't forget to use a binary mode if you transfer VCL files or their contents will be rendered unusable.

The 128 byte header has the following format:

byte number	purpose
0 - 3	ASCII String 'VCL1' which identifies the file type and version of the format.
4 - 7	The number of 12-byte records stored in this file, encoded as a big-endian (most significant byte first) 32-bit unsigned integer value.
8 - 23	Date and time when the recording started. Format: yyyymmddThhmmssZ, where yyyymmdd are year, month and day (e.g. '19940618'), hhmmss are hour, minute and second (e.g. '235959'). T is just the ASCII letter T, and Z is the ASCII letter Z if the time is UTC or a zero byte, if the time is local time. The digits are ASCII characters.
24 - 55	Name of the satellite or cable system from

which the recording was done. This is a zero terminated ASCII string with only characters between 20h and 7eh. As many zero bytes are appended as necessary for filling up the 32 bytes. The same format is also used for the next two text fields. Example: 'Astra'.

56 - 63 Name/number of the transponder from which the recording was done. Example: '08' for Sky One on Astra.

64 -127 Description of what has been recorded. Example: 'Star Trek: TNG, episode 123'

After the first 128 bytes follow as many 12 byte records as announced in bytes 4-7. Each record represents a 74h/78h Videocrypt protocol pair and consists of two fields. The first 4 bytes are the final 4 bytes of the 74h data part, the remaining 8 bytes are the data part of the corresponding 78h command. Four bytes of each 74h packet are enough to allow a card emulator to quickly and reliably synchronize with the queries of the decoder. The final four bytes of the 74h commands have been selected because of their high entropy (signature and checksum).

Impressum / Colophon

Kunstverein für die Rheinlande und Westfalen, Düsseldorf
Grabbeplatz 4
40213 Düsseldorf

Kathrin Bentele, Direktorin / Director
Gesa Hüwe, Kuratorische Assistenz / Curatorial Assistance
Hanna Welzel, Finanzen, Administration / Finance, Administration
Marius Comanns, Technische Leitung / Head of Technical Staff
Sigrid Konopka, Mitgliederbetreuung / Member's Desk
Aufbauteam / Installation Team: Valerie Buchow, Davit Chaganava, Katerina Matsagkos, Nina Nick, Myrto Vratsanou

Vorstand / Board: Lilli von Bodman, Georg Kulenkampff (Vorsitzender / Chairman), Rita McBride, Rudolf Dahmen, Martin Renker, Nicola Treyde, Renate Ulrich, Florian Wethmar

Übersetzung / Translation: Ben Caton
Grafikdesign / Graphic Design: Dan Solbach, Emma Kouassi

Besonderer Dank an / Special thanks to: Frank Berndt & Caroline Fuchs, Jack Callahan & Jeff Witscher, Alina Clavuot, Patrick Collins, Hans-Christian Dany, Cédric Eisenring, Fabian Flückiger, Patrick Frey, Isabelle Geller, Sophia Groebel, Matthew Hanson, Silvan Hillmann, Dennis Hochköppeler, Dr. Georg Jacobi, Andreas Koller, Kunstmuseum Liechtenstein, Thomas Losse-Müller, Frankie Mace, Dr. Friedemann Malsch, Sadie Plant, Jakob Pürling, Emanuel Rossetti, Teo Schifferli, Michael Schlösser, Hannes Schmidt, Sinan Stäheli, Wolf-Dieter Stoeffelmeier, Amikam Toren, Christian Wirtz, Marian Ziola

Der Kunstverein für die Rheinlande und Westfalen, Düsseldorf wird unterstützt durch / is supported by:

Landeshauptstadt Düsseldorf
de Haen-Carstanjen & Söhne
SONNEN HERZOG Wir leben Farbe.

Permanenter Partner des Kunstvereins / Permanent partner of the Kunstverein:

Stadtwerke Düsseldorf