INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

A note on replay attacks that violate privacy in electronic voting schemes

Ben Smyth — Véronique Cortier

N° 7643

Juin 2011

Thème SYM

ISSN 0249-6399 ISRN INRIA/RR--7643--FR+ENG

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

centre de recherche
NANCY - GRAND EST

A note on replay attacks that violate privacy in electronic voting schemes

Ben Smyth , Véronique Cortier

Thème SYM — Systèmes symboliques
Équipes-Projets Cassis

Rapport de recherche n° 7643 — Juin 2011 — 13 pages

Abstract: In our previous work, we have shown that the Helios 2.0 electronic voting protocol does not satisfy ballot independence and exploit this weakness to violate privacy; in particular, the Helios scheme is shown to be vulnerable to a replay attack. In this note we examine two further electronic voting protocols – namely, the schemes by Sako & Kilian and Schoenmakers – that are known not to satisfy ballot independence and demonstrate replay attacks that violate privacy.

Key-words: Ballot Independence, Ballot Secrecy, Electronic Voting, Privacy, Replay Attack, Vulnerability.

This research has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement n° 258865, project ProSecure, and the ANR-07-SeSur-002 AVOTÉ project.

Centre de recherche INRIA Nancy – Grand Est
LORIA, Technopôle de Nancy-Brabois, Campus scientifique,
615, rue du Jardin Botanique, BP 101, 54602 Villers-Lès-Nancy
Téléphone : +33 3 83 59 30 00 — Télécopie : +33 3 83 27 83 19

Une note sur l'utilisation des attaques par rejeu pour compromettre la confidentialité dans les protocoles de vote électronique

Résumé : Dans un résultat précédent, nous avons montré que le protocole de vote électronique Helios 2.0 ne garantissait pas l'indépendance des votes et que cela pouvait être utilisé pour compromettre la confidentialité des votes. Cette attaque repose en particulier sur le fait que le protocole Helios est vulnérable aux attaques par rejeu. Dans cette note, nous examinons le cas de deux autres protocoles de vote de la littérature – les protocoles Sako & Kilian et Schoenmakers – qui sont connus pour ne pas garantir l'indépendance des votes. Nous montrons comment cette vulnérabilité peut être à nouveau exploitée pour compromettre la confidentialité.

Mots-clés : vote électronique, indépendance des bulletins, confidentialité des votes, attaque par rejeu

1 Introduction

Paper-based elections derive ballot independence from physical characteristics of the real-world, for example, ballots are constructed in isolation inside polling booths and complete ballots are deposited into locked ballot boxes. By comparison, in a digital setting, ballots are sent using publicly readable communications channels and, in end-to-end verifiable elections, stored on a publicly readable bulletin board. Nevertheless, the provision of ballot independence is important to ensure privacy, as demonstrated in our earlier work [SC10, CS11] who exploit the lack of ballot independence in Helios 2.0 [AMPQ09] to violate ballot secrecy.

Informally, ballot independence is characterised by Gennaro [Gen95, §1.1] as follows.

Ballot independence. Observing another voter's interaction with the election system does not allow a voter to cast a *related* vote.

In addition to the apparent relationship between ballot independence and privacy, ballot independence is important because it prohibits the voting system from influencing a voter's behaviour; more formally, this requires that observation of the voting system (that is, observing interaction between participants) does not leak information that may affect a voter's vote.

The concept of privacy for electronic voting systems has been informally defined by the following properties [KR05, BHM08, DKR09].

Ballot secrecy. A voter's vote is not revealed to anyone.

Receipt freeness. A voter cannot gain information which can be used to prove, to a coercer, how she voted.

Coercion resistance. A voter cannot collaborate, with a coercer, to gain information which can be used to prove how she voted.

Other desirable properties of electronic voting systems include verifiability [JCJ02, Par07, KRS10].

Individual verifiability. A voter can check that her own ballot is published on the election's bulletin board.

Universal verifiability. Anyone can check that all the votes in the election outcome correspond to ballots published on the election's bulletin board.

Eligibility verifiability. Anyone can check that each ballot published on the bulletin board was cast by a registered voter and at most one ballot is tallied per voter.

The verifiability properties (also called *end-to-end verifiability* [JCJ02, CRS05, Adi06]) allow voters and election observers to verify – independently of the hardware and software running the election – that votes have been recorded, tallied and declared correctly.

We [SC10, CS11] have shown in Helios 2.0 it is possible to replay a voter's ballot (without knowing the vote contained within that ballot). This immediately violates ballot secrecy in an election with three voters. For example, consider the electorate Alice, Bob, and Mallory; if Mallory replays Alice's ballot, then Mallory can reveal Alice's vote by observing the election outcome and checking which candidate obtained at least two votes.

Contribution. We take two schemes presented at CRYPTO – namely, the protocols due to Sako & Kilian [SK94] and Schoenmakers [Sch99] – that are known not to satisfy ballot independence and show that these protocols are both vulnerable to replay attacks that violate privacy.

The study of Sako & Kilian [SK94] is interesting because it was one of the first electronic voting protocols to adopt the Fiat-Shamir heuristic to derive non-interactive proofs (this evolution was key for the development of end-to-end verifiable electronic voting systems). However, we will show that the application of the Fiat-Shamir heuristic compromises ballot secrecy. In particular, the interactive nature of zero-knowledge proofs guarantees ballot independence; whereas, non-interactive proofs, derived using the Fiat-Shamir heuristic, do not assure independence. This can be exploited by a replay attack to violate ballot secrecy.

In earlier work [SC10, CS11], we acknowledge that our attack against Helios may not be practical in large-scale elections, but it is particularly well suited to small-scale elections. The scheme by Schoenmakers [Sch99] was explicitly designed for small-scale elections (for example, boardroom elections) and, hence, we find it interesting to study the possibility of violating ballot secrecy in this setting. Once again, we violate privacy using a replay attack.

Related work. The concept of independence was introduced by Chor *et al.* [CGMA85] and the possibility of compromising security properties due to lack of independence has been considered, for example, by Chor & Rabin [CR87], Dolev, Dwork & Naor [DDN91, DDN00] and Gennaro [Gen95, Gen00]. In the context of electronic voting, Gennaro [Gen95] demonstrates that the application of the Fiat-Shamir heuristic in the Sako-Kilian electronic voting protocol [SK94] violates ballot independence, and Wikström [Wik06, Wik08] studies non-malleability for mixnets to achieve ballot independence. By comparison, we focus on the violation of ballot secrecy rather than ballot independence.

2 Sako-Kilian voting protocol

The Sako & Kilian [SK94] electronic voting scheme capitalises upon advances in cryptography to improve the Banaloh & Yung protocol [BY86]. In particular, the Fiat-Shamir heuristic is adopted to derive non-interactive proofs of knowledge.

2.1 Protocol description

The scheme is based upon a pair of *partially compatible homomorphic encryption* functions, that is, a pair of functions f_1, f_2 over $\mathbb{Z}_q$, where q is prime, such that for all $i, j \in \{1, 2\}$ the following properties are satisfied:

- $f_i(x + y) = f_i(x) \cdot f_i(y)$, where $x, y \in \mathbb{Z}_q$
- Distributions $(f_i(x), f_j(y))$ and $(f_i(x), f_j(x))$ are computationally indistinguishable, where x and y are chosen uniformly in $\mathbb{Z}_q$.

The Sako-Kilian voting protocol is defined for $m \in \mathbb{N}$ voters as follows.

Setup. Talliers $\mathcal{T}$ and $\mathcal{T}'$ publish public keys k and k' for a public key encryption scheme E (which need not be homomorphic).

Voting. Given vote $v_i \in \{-1, 1\}$, the voter generates nonces $x_i, x_i' \in \mathbb{Z}_q$ such that $v_i = x_i + x_i'$ and constructs her ballot as follows:

$$\begin{array}{rcl} Y_i & = & f_1(x_i) \\ Y_i' & = & f_2(x_i') \\ Z_i & = & E(k, x_i) \\ Z_i' & = & E(k', x_i') \end{array}$$

In addition, the voter is required to prove $x_i + x_i' \in \{1, -1\}$ in zero-knowledge. However, to avoid an interactive proof, the Fiat-Shamir heuristic is applied to derive a signature of knowledge σ_i. (For brevity we omit the construction of σ_i, see [SK94, Figure 1] for details.)

Tallying. Given ballots $Y_1, Y_1', Z_1, Z_1', \sigma_1, \ldots, Y_n, Y_n', Z_n, Z_n', \sigma_n$, tallier $\mathcal{T}$ decrypts each Z_i to recover $\hat{x}_i$ and checks $Y_i = f_1(\hat{x}_i)$, similarly, tallier $\mathcal{T}'$ decrypts Z_i' to recover $\hat{x}_i'$ and checks $Y_i' = f_1(\hat{x}_i')$; the talliers also check the signature of knowledge σ_i. The talliers publish $V = \sum_{i=1}^m \hat{x}_i$ and $V' = \sum_{i=1}^m \hat{x}_i'$, and the result is $T = V + V'$, which can be verified by checking $f_1(V) = \prod_{i=1}^m Y_i$ and $f_2(V') = \prod_{i=1}^m Y_i'$.

2.2 Attacking ballot secrecy

Ballot secrecy means a voter's vote is not revealed to anyone. We show that Sako-Kilian voting protocol does not satisfy this definition of ballot secrecy, by presenting a replay attack which allows an adversary to reveal a voter's vote.

Intuitively, an adversary may observe the ballot posted by a particular voter and recast this ballot by corrupting dishonest voters. The multiple occurrences of the voter's ballot will leak information in the tally and the adversary can exploit this knowledge to violate the voter's privacy. An informal description of the attack will now be presented in the case of three eligible voters.

2.2.1 Attack description.

Let us consider an election with three eligible voters who have identities id_1, id_2 and id_3. Suppose that voters id_1, id_2 are honest and id_3 is a dishonest voter controlled by the adversary. Further assume that the adversary has observed the ballot

$$Y_k, Y'_k, Z_k, Z'_k, \sigma_k$$

being cast by the voter whose privacy will be compromised.

Exploiting the absence of ballot independence. As shown by Gennaro [Gen95], an adversary can replay the ballot $Y_k, Y'_k, Z_k, Z'_k, \sigma_k$, thereby violating ballot independence. (The violation of ballot independence is due to the adversary's ability to cast the *same* vote as the honest voter.) Since the ballot was constructed by an honest voter, it is trivial to see that it will be considered valid by the talliers. We will now show how the lack of ballot independence can be exploited to violate privacy.

Violating privacy. The bulletin board will be constructed as follows

$$Y_1, Y'_1, Z_1, Z'_1, \sigma_1, Y_2, Y'_2, Z_2, Z'_2, \sigma_2, Y_k, Y'_k, Z_k, Z'_k, \sigma_k, V, V'$$

where $k \in \{1, 2\}$, $V = x_1 + x_2 + x_k$ and $V' = x'_1 + x'_2 + x'_k$. It follows from the protocol description that $v_i = x_i + x'_i$, where $i \in \{1, 2, k\}$, and the result $T = V + V' = v_1 + v_2 + v_k$. Since there will be at least two votes for the candidate voter id_k voted for, the voter's vote can be revealed: if $T \geq 2$, then $v_k = 1$; otherwise $v_k = -1$. It follows that the voter's privacy has been compromised; moreover, the vote of the remaining honest voter is $T - 2 \cdot v_k$.

3 Schoenmakers's voting protocol

The electronic voting scheme by Schoenmakers [Sch99] is based upon [CFSY96, CGS97] and aims to provide efficient small-scale elections. Ballot independence is explicitly not provided [Sch99, §5].

3.1 Protocol description

Given cryptographic parameters (G_q, g, h) and hash function $\mathcal{H}$, where G_q is a group of prime order q such that computing discrete logarithms is infeasible and g, h are distinct generators of G_q, let us recall the scheme for $n \in \mathbb{N}$ talliers and $m \in \mathbb{N}$ voters using some threshold $t \leq n$.

Setup. Each tallier $i \in n$ selects a private key $x_i \in_R \mathbb{Z}_q^*$ and computes the public part $y_i = h^{x_i}$.

Voting. The voter selects coefficients $\alpha_0, \ldots, \alpha_{t-1} \in_R \mathbb{Z}_q^*$ and constructs the polynomial ρ:

$$\rho(x) = \alpha_0 \cdot x^0 + \cdots + \alpha_{t-1} \cdot x^{t-1}$$

Given vote $v \in \{0, 1\}$, the ballot consists of the following components:

- Vote: $U = h^{\alpha_0 + v}$.
- Commitments: $C_j = g^{\alpha_j}$, where $0 \leq j \leq t-1$.
- Random shares: $Y_i = y_i^{\rho(i)}$, where $1 \leq i \leq n$.

In addition, the ballot includes a signature proof of knowledge [Ped91, CP93] demonstrating the correct construction of encrypted shares and a signature proof of knowledge [CDS94] demonstrating that $v \in \{0, 1\}$:

- Proof of correct construction. Let $X_i = \prod_{j=0}^{t-1} (C_j)^{i^j}$, where $1 \leq i \leq n$. For all $1 \leq i \leq n$, select a random nonce $w_i \in_R \mathbb{Z}_q^*$ and compute witnesses $a_i = g^{w_i}$, $b_i = y_i^{w_i}$. Derive the common challenge $c = \mathcal{H}(X_1, Y_1, a_1, b_1, \ldots, X_n, Y_n, a_n, b_n)$, and for all $1 \leq i \leq n$ compute response $r_i = w_i - c \cdot \rho(i)$.
- Proof of valid vote. Compute challenge $\hat{c}_{1-v} \in_R \mathbb{Z}_q^*$, response $\hat{r}_{1-v} \in_R \mathbb{Z}_q^*$ and witnesses $\hat{a}_{1-v} = g^{r_{1-v}} \cdot C_0^{\hat{c}_{1-v}}$ and $b_{1-v} = h^{r_{1-v}} \cdot (U/h^{1-v})^{\hat{c}_{1-v}}$. Select a random nonce $\hat{w} \in_R \mathbb{Z}_q^*$. Compute witnesses $\hat{a}_v = g^w$ and $\hat{b}_v = h^w$, challenge $\hat{c}_v = \mathcal{H}(\hat{a}_0, \hat{b}_0, \hat{r}_0, \hat{a}_1, \hat{b}_1, \hat{r}_1) - \hat{c}_{1-v}$ and response $r_v = w - \alpha_0 \cdot \hat{c}_v$.

To prevent a voter casting multiple ballots, the ballots are assumed to be associated with the voter's identity on the bulletin board.

Verification. For each ballot $U, C_0, \ldots, C_{t-1}, Y_1, \ldots, Y_n$ and associated proofs $a_1, b_1, r_1 \ldots, a_n, b_n, r_n$ and $\hat{a}_1, \hat{b}_1, \hat{c}_1, \hat{r}_1, \hat{a}_2, \hat{b}_2, \hat{c}_2, \hat{r}_2$, check for all $1 \leq i \leq n$ and $v \in \{0, 1\}$ that

$$\begin{array}{rclrclcl} a_i & = & g^{r_i} \cdot X_i^c & b_i & = & y_i^{r_i} \cdot Y_i^c & & \\ \hat{a}_v & = & g^{\hat{r}_v} \cdot C_0^{\hat{c}_v} & \hat{b}_v & = & h^{\hat{r}_v} \cdot (U/h^v)^{\hat{c}_v} & \hat{c}_0 + \hat{c}_1 & = & \mathcal{H}(\hat{a}_0, \hat{b}_0, \hat{a}_1, \hat{b}_1) \end{array}$$

where $X_i = \prod_{j=0}^{t-1} (C_j)^{i^j}$ and $c = \mathcal{H}(X_1, Y_1, a_1, b_1, \ldots, X_n, Y_n, a_n, b_n)$. (Observe $X_i = g^{\sum_{j=0}^{t-1} \alpha_j \cdot i^j} = g^{\rho(i)}$.)

Tallying. Given encrypted shares $Y_{1,1}, \ldots, Y_{1,n}, \cdots, Y_{m,1}, \ldots, Y_{m,n}$ of m voters, the homomorphic combination of encrypted shares Y_i^* is derived, where $1 \leq i \leq n$:

$$Y_i^* = \prod_{j=1}^{m} Y_{j,i}$$

Let ρ_j denotes the jth voter's secret polynomial. For all $1 \leq i \leq n$, each tallier derives the partial decryption $V_i = (Y_i^*)^{1/x_i}$; since $Y_i^* = y_i^{\sum_{j=1}^{m} \rho_j(i)} =$

$h^{x_i \cdot \sum_{j=1}^{m} \rho_j(i)}$, it follows that $V_i = h^{\sum_{j=1}^{m} \rho_j(i)}$. The talliers must also prove correctness of decryption; it is sufficient to prove equality between discrete logarithms $\log_h y_i$ and $\log_{V_i} Y_i^*$, we omit these details.

Given partial decryptions $V_1, \ldots, V_t$ from t talliers, we can compute $V = h^{\sum_{j=1}^{m} \alpha_{j,0}}$ as shown below, where $\alpha_{j,0}$ is the jth voter's first coefficient and, for simplicity, $t = n$. Let Lagrange coefficient $\lambda_i = \prod_{l \in \{1,\ldots,i-1,i+1,\ldots,n\}} \frac{l}{l-i}$, where $1 \leq i \leq n$.

$$\prod_{i=1}^{n} V_i^{\lambda_i} = \prod_{i=1}^{n} \left(h^{\sum_{j=1}^{m} \rho_j(i)} \right)^{\lambda_i} = h^{\sum_{j=1}^{m} \left(\sum_{i=1}^{n} \rho_j(i) \cdot \lambda_i \right)} = h^{\sum_{j=1}^{m} \rho_j(0)} = V$$

The result $T = \sum_{j=1}^{m} v_j$ can be derived as follows, where v_j is the jth voter's vote.

$$\log_h \prod_{j=1}^{m} U_j - \log_h V = \log_h h^{\sum_{j=1}^{m} \alpha_{j,0} + v_j} - \log_h h^{\sum_{j=1}^{m} \alpha_{j,0}} = \log_h h^{\sum_{j=1}^{m} v_j} = T$$

Although the computation of discrete logarithms is hard in general, given the restricted domain $[0, m]$, the result T can be computed efficiently; for example, the complexity is $O(m)$ by linear search or $O(\sqrt{m})$ using the baby-step giant-step algorithm [Sha71] (see also [LL90, §3.1]).

3.2 Attacking ballot secrecy

We show that Schoenmakers's voting protocol does not satisfy ballot secrecy, by presenting a replay attack which allows an adversary to reveal a voter's vote. Intuitively, an adversary may identify a voter's ballot on the bulletin board (since it is linked to the voter's identity) and recast this ballot by corrupting dishonest voters. As previously discussed, the multiple occurrences of the voter's ballot will leak information in the tally and the adversary can exploit this knowledge to violate the voter's privacy. An informal description of the attack will now be presented in the case of three eligible voters.

3.2.1 Attack description.

Let us consider an election with n talliers and three eligible voters who have identities id_1, id_2 and id_3. Suppose that voters id_1, id_2 are honest and id_3 is a dishonest voter controlled by the adversary. Further assume that the honest voters have cast their ballots. The bulletin board entries are as follows:

$$id_1, e_1, spk_1, spk'_1$$
$$id_2, e_2, spk_2, spk'_2$$

where for $i \in \{1, 2\}$ we have

$$\begin{array}{lcl} e_i & = & U_i, C_{i,0}, \ldots, C_{i,t-1}, Y_{i,1}, \ldots, Y_{i,n} \\ spk_i & = & a_{i,1}, b_{i,1}, r_{i,1} \ldots, a_{i,n}, b_{i,n}, r_{i,n} \\ spk'_i & = & a_{i,1}, \hat{b}_{i,1}, \hat{c}_{i,1}, \hat{r}_{i,1}, \hat{a}_{i,2}, \hat{b}_{i,2}, \hat{c}_{i,2}, \hat{r}_{i,2} \end{array}$$

That is, e_i contains the ith voter's vote U_i, commitments $C_{i,0}, \ldots, C_{i,t-1}$ and random shares $Y_{i,1}, \ldots, Y_{i,n}$; spk_i demonstrates that the random shares are correctly formed; and spk'_i demonstrates that U_i contains either 0 or 1.

Exploiting the absence of ballot independence. The adversary observes the bulletin board and selects e_k, spk_k, spk'_k where $k \in \{1, 2\}$ and id_k is the voter whose privacy will be compromised. The adversary submits the ballot e_k, spk_k, spk'_k and it immediately follows that the bulletin board is composed as follows:

$$id_1, e_1, spk_1, spk'_1$$
$$id_2, e_2, spk_2, spk'_2$$
$$id_3, e_k, spk_k, spk'_k$$

It is trivial to see that each bulletin board entry is valid; that is, spk_1, spk'_1, spk_2, spk'_2, spk_k, spk'_k are all valid signatures of knowledge. We have shown that the protocol does not satisfy ballot independence (observing another voter's interaction with the election system allows a voter to cast the *same* vote), and this will now be exploited to violate privacy.

Violating privacy. The partial decryptions of the homomorphic combination of encrypted shares can be used to reveal the result $T = \log_h h^{v_1+v_2+v_k}$, where $k \in \{1, 2\}$ and v_1, v_2 are the votes of honest voters. Since there will be at least two votes for the candidate voter id_k voted for, the voter's vote can be revealed: if $T \geq 2$, then $v_k = 1$; otherwise $v_k = 0$. It follows that the voter's privacy has been compromised; moreover, the vote of the remaining honest voter is $T - 2 \cdot v_k$.

4 Discussion

We have informally shown that the protocols due to Sako & Kilian [SK94] and Schoenmakers [Sch99] are vulnerable to a replay attack which violates ballot secrecy. In this section we briefly discuss how application of the Fiat-Shamir heuristic may erode privacy, examine how the attacks can be extended beyond the three voter setting, and explore the attacks in the context of standard security definitions.

Independence and the Fiat-Shamir heuristic. The interactive nature of zero-knowledge proofs guarantees independence; by comparison, non-interactive proofs, derived using the Fiat-Shamir heuristic, do not assure independence. As a consequence, application of the Fiat-Shamir heuristic may compromise the security of cryptographic protocols and this paper has shown how ballot secrecy in electronic voting schemes can be violated.

Generalised attacks against ballot secrecy. Our attacks demonstrate that the ballot of an arbitrary voter can be replayed by any other voter. In general, this does not reveal the voter's vote. However, some information is leaked, and

colluding voters can replay sufficiently many ballots to leak the voter's vote. Moreover, we have previously shown that there is a realistic threat from a small coalition of dishonest voters [SC10, CS11].

Violating standard definitions of ballot secrecy. Intuitively, it should follow that the protocols due to Sako & Kilian [SK94] and Schoenmakers [Sch99] cannot satisfy ballot secrecy in formal settings defined by Kremer *et al.* [KR05, DKR09] and Backes, Hriţcu & Maffei [BHM08]. These privacy definitions consider two voters $\mathcal{A}$, $\mathcal{B}$ and two candidates t, t'. Ballot secrecy is captured by the assertion that an adversary (controlling arbitrary many dishonest voters) cannot distinguish between a situation in which voter $\mathcal{A}$ votes for candidate t and voter $\mathcal{B}$ votes for candidate t', from another one in which $\mathcal{A}$ votes t' and $\mathcal{B}$ votes t. This can be expressed by the following equivalence.

$$\mathcal{A}(t) \mid \mathcal{B}(t') \approx \mathcal{A}(t') \mid \mathcal{B}(t)$$

Formally proving that these protocols do not satisfy these definitions is beyond the scope of this paper. However, informally this result can be trivially witnessed and we deduce either: these definitions are too strong, or there are indeed weaknesses in the protocols we have studied.

References

[Adi06] Ben Adida. *Advances in Cryptographic Voting Systems*. PhD thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 2006.

[AMPQ09] Ben Adida, Olivier de Marneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing a University President Using Open-Audit Voting: Analysis of Real-World Use of Helios. In *EVT/WOTE'09: Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*. USENIX Association, 2009.

[BHM08] Michael Backes, Cătălin Hriţcu, and Matteo Maffei. Automated Verification of Remote Electronic Voting Protocols in the Applied Pi-calculus. In *CSF'08: 21st Computer Security Foundations Symposium*, pages 195–209. IEEE Computer Society, 2008.

[BY86] Josh Cohen Benaloh and Moti Yung. Distributing the Power of a Government to Enhance the Privacy of Voters. In *PODC'86: 5th Principles of Distributed Computing Symposium*, pages 52–62. ACM Press, 1986.

[CDS94] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In *CRYPTO'94: 14th International Cryptology Conference*, volume 839 of *LNCS*, pages 174–187. Springer, 1994.

[CFSY96] Ronald Cramer, Matthew K. Franklin, Berry Schoenmakers, and Moti Yung. Multi-Autority Secret-Ballot Elections with Linear Work. In *EUROCRYPT'96: 15th International Conference on the Theory and Applications of Cryptographic Techniques*, volume 1070 of *LNCS*, pages 72–83. Springer, 1996.

[CGMA85] Benny Chor, Shafi Goldwasser, Silvio Micali, and Baruch Awerbuch. Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults. In *FOCS'85: 26th Foundations of Computer Science Symposium*, pages 383–395. IEEE Computer Society, 1985.

[CGS97] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Scheme. In *EUROCRYPT'97: 16th International Conference on the Theory and Applications of Cryptographic Techniques*, volume 1233 of *LNCS*, pages 103–118. Springer, 1997.

[CP93] David Chaum and Torben P. Pedersen. Wallet Databases with Observers. In *CRYPTO'92: 12th International Cryptology Conference*, volume 740 of *LNCS*, pages 89–105. Springer, 1993.

[CR87] Benny Chor and Michael O. Rabin. Achieving Independence in Logarithmic Number of Rounds. In *PODC'87: 6th Principles of Distributed Computing Symposium*, pages 260–268. ACM Press, 1987.

[CRS05] David Chaum, Peter Y. A. Ryan, and Steve Schneider. A Practical Voter-Verifiable Election Scheme. In *ESORICS'05: 10th European Symposium On Research In Computer Security*, volume 3679 of *LNCS*, pages 118–139. Springer, 2005.

[CS11] Véronique Cortier and Ben Smyth. Attacking and fixing Helios: An analysis of ballot secrecy. In *CSF'11: 24th Computer Security Foundations Symposium*. IEEE Computer Society, 2011. To appear.

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-Malleable Cryptography. In *STOC'91: 23rd Theory of computing Symposium*, pages 542–552. ACM Press, 1991.

[DDN00] Danny Dolev, Cynthia Dwork, and Moni Naor. Nonmalleable Cryptography. *Journal on Computing*, 30(2):391–437, 2000.

[DKR09] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security*, 17(4):435–487, July 2009.

[Gen95] Rosario Gennaro. Achieving independence efficiently and securely. In *PODC'95: 14th Principles of Distributed Computing Symposium*, pages 130–136. ACM Press, 1995.

[Gen00] Rosario Gennaro. A Protocol to Achieve Independence in Constant Rounds. *IEEE Transactions on Parallel and Distributed Systems*, 11(7):636–647, 2000.

[JCJ02] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-Resistant Electronic Elections. Cryptology ePrint Archive, Report 2002/165, 2002.

[KR05] Steve Kremer and Mark D. Ryan. Analysis of an Electronic Voting Protocol in the Applied Pi Calculus. In *ESOP'05: 14th European Symposium on Programming*, volume 3444 of *LNCS*, pages 186–200. Springer, 2005.

[KRS10] Steve Kremer, Mark D. Ryan, and Ben Smyth. Election verifiability in electronic voting protocols. In *ESORICS'10: 15th European Symposium on Research in Computer Security*, volume 6345 of *LNCS*, pages 389–404. Springer, 2010.

[LL90] Arjen K. Lenstra and Hendrik W. Lenstra Jr. Algorithms in Number Theory. In Jan van Leeuwen, editor, *Handbook of Theoretical Computer Science, Volume A: Algorithms and Complexity*, chapter 12, pages 673–716. MIT Press, 1990.

[Par07] Participants of the Dagstuhl Conference on Frontiers of E-Voting. Dagstuhl Accord. `http://www.dagstuhlaccord.org/`, 2007.

[Ped91] Torben P. Pedersen. A Threshold Cryptosystem without a Trusted Party. In *EUROCRYPT'91: 10th International Conference on the Theory and Applications of Cryptographic Techniques*, number 547 in LNCS, pages 522–526. Springer, 1991.

[SC10] Ben Smyth and Véronique Cortier. Attacking and fixing helios: An analysis of ballot secrecy. Cryptology ePrint Archive, Report 2010/625, 2010.

[Sch99] Berry Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic voting. In *CRYPTO'99: 19th International Cryptology Conference*, volume 1666 of *LNCS*, pages 148–164. Springer, 1999.

[Sha71] Daniel Shanks. Class number, a theory of factorization and genera. In *Number Theory Institute*, volume 20 of *Symposia in Pure Mathematics*, pages 415–440. American Mathematical Society, 1971.

[SK94] Kazue Sako and Joe Kilian. Secure Voting Using Partially Compatible Homomorphisms. In *CRYPTO'94: 14th International Cryptology Conference*, volume 839 of *LNCS*, pages 411–424. Springer, 1994.

[Wik06] Douglas Wikström. Simplified Submission of Inputs to Protocols. Cryptology ePrint Archive, Report 2006/259, 2006.

[Wik08] Douglas Wikström. Simplified Submission of Inputs to Protocols. In *SCN'08: 6th International Conference on Security and Cryptography for Networks*, volume 5229 of *LNCS*, pages 293–308. Springer, 2008.

Centre de recherche INRIA Nancy – Grand Est
LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Grenoble – Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier
Centre de recherche INRIA Lille – Nord Europe : Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq
Centre de recherche INRIA Paris – Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Saclay – Île-de-France : Parc Orsay Université - ZAC des Vignes : 4, rue Jacques Monod - 91893 Orsay Cedex
Centre de recherche INRIA Sophia Antipolis – Méditerranée : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399